**Confidential**

Internal Audit Directorate,
Health Service Executive,
63-64 Adelaide Road,
Dublin 2.

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

# Report

| | |
|---|---|
| **To:** | Mr. Tony McNamara, CEO, Cork University Hospital (CUH) Group |
| **From:** | Joe Ryan, Assistant National Director, ICT Audit, HSE |
| **Subject:** | Cork University Hospital IT General Controls (ITGC) |
| **Ref:** | **ICTA014ISDA0712** |
| **Report Prepared by:** | Alex Burnham, Auditor, Mazars |
| **Report Reviewed by:** | Roberto Franconi, Manager, Mazars |
| **Report Approved by:** | Dera McLoughlin, Partner, Mazars<br>Joe Ryan, Assistant National Director, ICT Audit, HSE |
| **Date Report Issued:** | **10th July, 2012.** |
| **Distribution List:** | Mr. Mike O'Regan, ICT Manager, CUH;<br>Mr. John Lehane, ICT Technical Support Manager, HSE South;<br>Mr. Gerard Hurl, National Director of ICT, HSE;<br>Mr. Fran Thompson, A/Head National ICT, HSE;<br>Mr. Michael Flynn, National Director of Internal Audit, HSE;<br>Mr. Liam Woods, National Director of Finance, HSE;<br>Ms. Valerie Plant, Assistant National Director of Finance, HSE;<br>Audit Committee. |

# Table of Contents

# Section 1 - Executive Summary

## 1.1. Audit Objectives

This audit was carried out based on the following control objectives:

- Existence and adequacy of appropriate hospital ICT governance structures and processes;
- Compliance of security practices with HSE ICT policies;
- Existence and adequacy of controls to protect sensitive patient data at network level;
- Existence and adequacy of controls to protect sensitive patient data at local hospital application level;
- Existence and adequacy of controls in place to ensure the effective operational performance of ICT;
- Adequacy of the methodology employed and integrity of patient records arising from the combination of the PAS records of the CUH, South Infirmary and Mercy Hospitals.

## 1.2. Key Findings

Analysis of Key Findings

| | National | Regional | Local | Total |
|---|---|---|---|---|
| **High** | 2 | 2 | 5 | 9 |
| **Medium** | 4 | 1 | 20 | 25 |
| **Low** | 1 | - | 7 | 8 |
| **Total** | **7** | **3** | **32** | **42** |

Key Findings - Ranking Priority – High

**National**

1. **Integrated Patient Management System (IPMS) Password Controls:** [redacted]

2. **Presence of Unauthorised Data Disk Shares in CUH & South Region:** [redacted]

[redacted]

**Regional**

3. **Information Security Governance:** An ICT Governance Framework to ensure that access to the hospital sensitive data is controlled and restricted to only authorised staff is not in place. The auditors noted that an ICT Governance Group was established in the South Region, however, a number of gaps were noted and are detailed later in this report.

4. **Access Controls on the [redacted] Childcare System:** [redacted]

**Local**

5. **Passwords Disclosure:** [redacted]

6. **Network Passwords Requirements:** [redacted]

7. **IPMS User Access Management:** [redacted]

[redacted]

8. **Sensitive Data Accessible on Shares:** [redacted]

9. **ICT Budgeting:** At present no formal budget is prepared by ICT or by the hospital on the basis of existing commitments and known expenditure, and at the date of the audit (March 2012) no ICT budget had been established for 2012. In addition, it is apparent that a number of specific ICT expenditure items are not accounted for under the ICT budget for 2011, rather they are reported under other cost headings. It is not clear whether they are reported under the ICT Expenditure – Start of Year Submission' (to the ICT Control Section, CMOD, Department of Finance) by National ICT.

Key Findings - Ranking Priority – Medium

**National**

10. **ICT Key Performances Indicators:** The auditors noted that there are no Service Level Agreements (SLAs) agreed between the business and the ICT department. ICT performance is not measured against specific / defined targets.

11. **Reporting Structures, Roles and Responsibilities:** A lack of clarity between the roles and responsibilities of the local ICT department in CUH and the HSE South Region ICT department was apparent in the course of the audit., Although meetings are held between the local ICT department within CUH and the HSE South Region ICT department, it appears that a formal reporting structure is not in place. It was also understood that the CUH ICT department had little or no input into the National HSE ICT Strategy.

12. [redacted] Limited resilience is in place to protect CUH critical servers and data in the event of damage to the CUH data centre due to the lack of resilience in [redacted]. [redacted]

13. **Notepad found in the CUH car park:** While this is an out of scope finding, the auditors are obliged to note and notify that a folder containing sensitive employee information was found by the auditors on the machine for paying the parking tickets.

**Regional**

14. **Intrusion Detection System (IDS):** [redacted]

**Local**

15. **ICT Steering Committee:** Whilst an ICT Steering Committee is in place, the group would only appear to be project focused. The Steering Committee does not provide oversight or review of: ICT standard performance metrics or targets; ICT operational budgets, reporting against budget; data management and Data Protection; security management, or policy compliance.

16. **Reporting on Policy Compliance or Exceptions:** A process to formally report on the implementation of, or compliance with, National ICT Security Policies is not in place. Where non-compliance with the policies existed, these gaps had not been formally reported to the National ICT Directorate as required in the policies. As a consequence, hospital management cannot provide an adequate level of assurance that the National ICT Security Policies are implemented, as requested by the HSE's CEO in his communication to all National Directors regarding Data Protection on the 10th August 2011.

17. **Business Staff Awareness:** A number of business users were interviewed by the auditors to assess their knowledge of the Encryption, Remote Access, Access Control, and Passwords Standards National ICT Policies. Staff were either not aware of any of the policies (50%), aware of the existence of the policies but not of their content (31%), while 19% were aware of and acknowledge having read, at most, one of the policies. All users informed the auditors that they have received no training in relation to any of the policies and have not been asked to accept them. While the policies may be rolled out at a National level, there is little evidence to suggest they are being implemented at a local hospital level and user awareness of the contents and controls outlined in the policies is poor.

18. **ICT Staff Awareness:** ICT staff have a mixed level of awareness of the National ICT Policies. The audit found that although CUH ICT management and staff are aware that National ICT Policies exist they are not aware of their content, the audit revealed that there is no direct communication of these policies to CUH ICT staff. Staff have had no training on the use and/or application of these policies. CUH ICT does not monitor the level of compliance with the policies and there is no requirement to report compliance levels to HSE ICT.

19. **Active Directory Joiners Process Gaps:** There is no formal / documented User Access Management procedure that documents the process for creating active directory accounts and issuing network rights in line with HSE policy and business requirements. The National HSE Systems Access Request Form is

not used, a local application form is in place within CUH that requires Line Managers' authorisation. However, the auditor tested a sample of new members of staff selected from a report provided by HR and determined that 13.3% of the forms were not authorised (i.e. not signed by Line Managers). [redacted]

20. **Leavers Process Gaps:** A formally documented procedure for revoking the access of leavers and movers is not in place. A process is in place to disable all accounts that have been inactive for a period of [redacted] days or more, however, this process is not in line with the Access Control Policy as that indicates [redacted] days.

21. **Movers Process Absence:** A process is not in place in CUH to ensure that network access such as [redacted] shared folders and specialist applications granted to a member of CUH staff is revoked when they change role within the hospital.

22. **Active Directory (AD) Generic Accounts:** [redacted]

23. **AD Administrators:** [redacted]

24. **Active Users Reviews:** The threshold for identifying inactive accounts is not in line with the HSE Access Control Policy threshold of [redacted] days. [redacted] network accounts were identified as being inactive for over [redacted] days. While a process is in place for removing inactive accounts, through substantive testing the auditors were able to determine that [redacted] accounts have been inactive for over [redacted] days and have not been moved to the Disabled OU (Organisational Unit) as required under CUH procedure.

25. **Users' Access Rights Reviews:** A formal process for the review of the level of access granted to users on the network is not in place within CUH. The auditor was unable to identify information owners for each department who are responsible for reviewing access rights within their department. This does not meet the requirements of the HSE Access Control Policy that states that the Information Owners or their nominees must continually monitor access to their information systems and that they must perform quarterly reviews of the systems they are responsible for.

26. **Third Party AD Administrators:** [redacted]

27. **IPMS Administrative Access:** [redacted]

28. **IPMS Data Extraction Facilities:** [redacted]

29. **Network Audit Logs:** [redacted]

30. **Server Security Patches:** [redacted]

31. **Use of USB keys:** [redacted]

[redacted]

32. **Presence of Possible Duplicates:** Data analysis was performed on the merged PAS databases of the CUH, South Infirmary and Mercy Hospitals. The data analysis performed on over 1.241 million records indicates the presence of 239,594 possible duplicate records (19.30% of the total) that need to be analysed by the Medical Records staff to assess whether these records could be merged or not. The auditors acknowledge that a similar process was carried out by local management; a proposal was drafted and at the time of audit this was being reviewed.

33. **Data Collection Process:** The data analysis performed on over the 22,302 records entered in IPMS after the data migration process was completed shows the presence of records that appear to be duplicates or that do not contain all key fields filled-in, the auditors used the 1st of August 2011 as a cut-off day. It appears that 5,530 records (33%) entered after the date of data migration contain errors.

34. **ICT Helpdesk Performance:** The performance of the CUH ICT Helpdesk is not measured. CUH ICT management informed the auditor that 3 Service Level Agreements exist between ICT and the Bantry General Hospital, the Mallow General Hospital, and the Blood Transfusion Service; however, ICT is not formally committed to respond to issues with defined times and service standards. Service desk performance statistics/reports are neither produced nor communicated to Senior Management.

Key Findings - Ranking Priority - Low

Findings rated as low priority are detailed in section 2.7 of this report.

## 1.3. Management Comment

There are significant issues raised within this audit which require a lot of input from outside of Cork University Hospital, and the focus from within CUH is on delivering on what can be achieved within the resources available and the constraints that exist with regards to scope of responsibility. We will liaise with HSE ICT in relation to certain findings where the onus of responsibility for those findings lies with them.

The ICT Department within Cork University Hospital is very small (7.5WTE) in comparison with other major academic teaching hospitals. We do have additional project resources (2 WTE) made available by HSE ICT and we depend heavily on HSE ICT Infrastructure & Operations (HSE South) for the delivery of practically all infrastructure and infrastructure support. This service within the HSE South is also very small in numbers and they also have to provide input in to a lot of national I&O projects on top of their work in the HSE South.

Cork University Hospital values and recognises the role that ICT can play in a large modern healthcare organisation, however, we are constrained in terms of how we can resource this service. There are a large number of projects involving ICT which are currently active and there is a real issue around balancing resources and priorities to deliver on these projects whilst at the same time dealing with the findings of the

internal audit. The actions against the findings have, by necessity, realistic delivery time frames. This will require us to recognise and carry the identified risk against the findings until we can achieve a resolution.

There are a number of common themes and inter-relationships across and between the findings and there is therefore some commonalty in terms of the management response and the corrective actions. There are two key actions arising out of this whole exercise which will help in the overall ICT governance / controls arena – 1) the production of a hospital ICT Management Plan and 2) the production of an ICT Handbook for line managers.

The EMB receive an ICT briefing from the ICT Manager every three months as part of the existing hospital governance framework, and the actions arising out of this audit will be reviewed by the EMB at these regular reviews.

## 1.4. Audit Opinion

The auditors noted the existence of management controls and initiatives including the migration of data to a managed storage area network. However, the overall assessment of the IT General Control environment in place in Cork University Hospital can be considered to be inadequate due to the significant number of high and medium findings identified at national, regional and local hospital level during the audit. There are a significant number of gaps in relation to the management and protection of sensitive data, which is stored in the ICT resources managed within the Hospital (e.g. applications and network).

This opinion reflects the fact that although the audit took place at local hospital level, some of the ICT services within the scope of review are not provided directly by Cork University Hospital ICT, but are the responsibility of HSE South ICT.

The audit opinion also considers the fact that at the date of the audit, the suite of National ICT Policies has been in existence across the HSE for two years however the implementation of the suite of policies within the hospital has not been fully realised. The controls specified in the suite of National ICT Policies represent best practice and a stronger level of control than that which was in place in Cork University Hospital at the time of the audit.

## 1.5. Acknowledgement

Internal Audit wishes to formally acknowledge the excellent co-operation and courtesy afforded to them during this audit.

**Dera McLoughlin**
**Partner, Mazars**

**Joe Ryan**
**Assistant National Director, HSE**

**Date**

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Internal Audit Directorate,
Health Service Executive,
63-64 Adelaide Road,
Dublin 2.

# Section 2 - Main Report

**Cork University Hospital IT General Controls (ITGC)**

**Ref: ICTA014ISDA0712**

## 2.1. Introduction

This audit was carried out as part of the agreed audit plan for the HSE for 2012. Mazars was contracted by the HSE's Internal Audit Directorate to undertake an internal audit of the IT General Controls in place in Cork University Hospital (CUH).

## 2.2. Background

CUH is one of the largest University teaching hospitals in Ireland. Within the services offered by the hospital there are Cancer Services, Cardiac Services (Heart), General Surgery / Vascular Surgery / Urology, Paediatrics (Children's Services), Psychiatry and Radiology (X-Ray). It is also known as the Cork Regional Hospital and primarily treats patients from Cork and Kerry which have a combined population of more than 600,000 people.

CUH ICT manage and support the Hospital's main ICT resources including the critical combined patient administration system (PAS) IPMS application which, after a significant data migration project to merge 3 separate databases, is used and accessed by Cork city's Voluntary (non-HSE) hospitals, Mercy University Hospital (MUH) and the South Infirmary Victoria University Hospital (SIVUH).

HSE South ICT manages and provides the following ICT services to the Hospital:

- Active Directory infrastructure;
- Network management.

## 2.3. Audit Objectives

This audit was carried out based on the following control objectives:

- Existence and adequacy of appropriate hospital ICT governance structures and processes;

- Compliance of security practices with HSE ICT policies;
- Existence and adequacy of controls to protect sensitive patient data at network level;
- Existence and adequacy of controls to protect sensitive patient data at local hospital application level;
- Existence and adequacy of controls in place to ensure the effective operational performance of ICT;
- Examine combined Patient Administration System (PAS) of CUH, South Infirmary and Mercy Hospitals - methodology and record integrity.

## 2.4. Audit Scope

The purpose of this audit was to determine the existence and adequacy of controls in place which support the management of ICT and which protect data within the Cork University Hospital only.

This scope of the audit focussed on a detailed assessment of the controls in place in the following areas:

- ICT governance;
- HSE ICT policies;
- Patient data security at network level;
- Patient data security at application level;
- Operational performance of ICT;
- Patient record integrity and approach to the migration of data from legacy to current PAS systems in CUH.

## 2.5. Audit Methodology

The audit work was performed in accordance with the auditors' understanding of the proper interpretation of the law and in accordance with best practice as represented by:

- Institute of Internal Audit (IIA);
- Information Systems Audit and Control Association (ISACA) – COBIT standards.

Target Maturity Level

The long term goal of the HSE is to move to a control maturity level of 4: "Managed and Measurable". The audit approach was aligned with this objective and was conducted against a target maturity level of 2 ("repeatable but intuitive") as specified by COBIT. Level 2 definition states that "processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely".

Local, Regional or National Deployment Model

This was conducted at a local level in Cork University Hospital (CUH) only.

ICT Audit Intervention Model

A level 5 intervention model was adopted. Detailed testing of certain areas was performed where the cause and effect is direct, and where the impact and the likelihood of a risk occurring was considered to be high.

## 2.6. Ranking of Findings

1. The main findings, control weaknesses noted or suggested areas for improvement are ranked as high, medium or low and are dealt with in order of priority in the following paragraphs.

2. The rankings used are described below:

| | |
|---|---|
| **High** | Identifies a control area which poses a key risk to the HSE and/or its service users and clients (e.g. strategic, operational, financial (including VFM) or reputational) and where serious control weaknesses are preventing the effective management of that risk and should be addressed immediately. |
| **Medium** | Identifies a weakness in control which, while its implications are not as serious as the above, or the control itself not as fundamental to the operation of the system, nevertheless represents a risk to the HSE and needs to be addressed in order to reduce that risk to an acceptable level. These should be dealt with in the short term. |
| **Low** | Identifies a procedure or control that needs improvement in order to operate in a more effective way and should be addressed in the short to medium term. |

Some risks identified will have implications for the HSE nationally and therefore require consideration on a broader basis. Any risks identified that may have national implications will be denoted with an **(N)** e.g. High (N), Medium (N) and Low (N).

## 2.7. Key Findings, Risks and Recommendations

Listed hereunder are the findings, risks and recommendations associated with this report together with a time schedule for the implementation of the recommendations.

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **1. Integrated Patient Management System (IPMS) Password Controls**<br>Password controls in place on the IPMS system are not in line with the ICT Passwords Standards Policy. The following gaps are apparent:<br>• [redacted]<br>**Ranking: High (N)** | In the absence of strong password controls to the IPMS, there is an increased risk of unauthorised access to the system. [redacted] | [redacted] | This cannot be viewed in isolation as users within CUH access a number of systems as part of their daily working routine. The complete rectification of this requires the implementation of the Self-Service component of the [redacted] Password Manager. This has been discussed between CUH ICT and HSE South I&O and a plan will be drawn up for the implementation. This will need to go through local change control procedure and will require extensive testing prior to implementation in Production environment. This will facilitate the enforcement of required password controls. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | [redacted]<br><br>Where these requirements cannot be enforced (e.g. due to technical limitations of the application) then a non-compliance exception should be raised to the HSE's National Director of ICT.<br><br>**Responsible Officer:** Information Services Manager CUH / IT Technical Support Manager<br>**Implementation date:** Nov 2012 | |
| **2. Presence of Unauthorised Data Disk Shares in CUH & South Region**<br>Unauthorised shares were found on HSE South [redacted] | Where access is not restricted, there is a risk of unauthorised and inappropriate access to sensitive and personal information through file shares on the network. This risk is increased | The Organisation should restrict access to network locations, shares, folders and files containing sensitive data to authorised users only. This access should be granted in line with business roles and | This has been on the HSE South I&O agenda for some time and we have been working with them on the rationalisation of 'shares' within CUH. We will complete the re-organisation of server based shares in CUH by the end of July 2012. The issue with [redacted] shares is in identification of same – we will continue to work on this and remove when identified and |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| [redacted]<br><br>**Ranking: High (N)** | when everyone is granted access to the shares.<br><br>Where access is not restricted, there is a risk of unauthorised and inappropriate access to sensitive and personal information through file shares on the network. This risk is increased when "everyone" is granted access to the shares (often this is the standard setting for Windows shares).<br><br>[redacted] | responsibilities, and reviewed periodically.<br><br>Staff should be instructed as to use only shared folders created on a centralised server build up for this purpose.<br><br>Existing shares should be moved on the centrally managed servers used for files sharing (as they are subject to regular backups and adequate physical access controls), while users should be prevented (e.g. technically) from being able to create shares [redacted].<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** July 2012 | AD group policy will be applied to prevent creation of new shares.<br><br>Shares elsewhere in the HSE South will have to be dealt with by the individual units and their relevant ICT support personnel.<br><br>All new shares within CUH will be controlled through CUH ICT. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | [redacted]<br><br>Moreover, shares not saved on central server may not be backed up on a regular basis, and where data is inadvertently deleted there is a risk of the data not being restored. | | |
| **3. Information Security Governance**<br>An ICT Governance Framework to ensure that access to the hospital sensitive data is controlled and restricted to the only authorised staff is not in place. The auditors noted that an ICT Governance Group was established in the South Region, however it appears that:<br>• Responsibility for enforcing IT security is not formally assigned;<br>• Data owners or business owners are not identified for the internal systems / applications;<br>• Data access is not formally reviewed;<br>• A data classification schema (or similar document) that informs Information Owners on the categories of data (e.g. sensitive personal, HSE confidential, | Information security may not be enforced within the hospital. This may result in:<br>• Breach of the Data Protection Act(s) where personal data disclosures take place;<br>• Patients' erroneous medical treatments where patient data integrity is compromised. | An ICT Governance Framework should be put in place to ensure that access to the hospital sensitive data is controlled and restricted to only authorised staff. At a minimum the following should be defined within the framework:<br>• Assign responsibility for enforcing ICT security;<br>• Identify data owners and business owners | CUH will define an Information Governance Policy as part of an overall ICT Governance Framework in accordance with recently published HIQA guidelines. We will need to liaise with other entities in doing this and ultimately will need a shared Information Governance Policy with those entities. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| etc.) and ICT custodians about the level of protection required to protect data was not in place;<br>• A proactive security management program at an organisational level was not evident during the course of the audit, i.e. monitoring, testing and reporting of compliance against standards and policies;<br>• Management at hospital level with responsibility for implementing policies are not required to report on ICT security policy compliance.<br><br>**Ranking: High** | | for all key internal systems / applications;<br>• Perform formal reviews on a regular basis of the level of access granted to sensitive data;<br>• A data classification schema (or similar document) is introduced for the categorisation of data (e.g. sensitive, personal, HSE confidential, medical, etc.) and the level of protection required to protect the data is defined;<br>• A proactive security management program at an organisational level is defined (i.e. for the monitoring, testing and reporting of compliance against | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | standards and policies);<br>• Management at hospital level are assigned responsibility for implementing policies and for reporting on ICT security policy compliance.<br><br>**Responsible Officer:** CUH Executive Management Board<br>**Implementation date:** Dec 2012 | |
| **4. Access Controls on the [redacted] Childcare System**<br>[redacted] | [redacted] | [redacted] | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| [redacted]<br><br>**Ranking: High** | [redacted] | [redacted]<br><br>**Responsible Officer:** HSE | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | South [redacted] System Manager<br>**Implementation date:**<br>June 2012 | |
| **5. Passwords Disclosure**<br>[redacted] | [redacted] | [redacted] | This will be achieved in conjunction with the implementation of the resolution of key finding 1. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| [redacted]<br><br>**Ranking: High** | [redacted] | [redacted]<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Nov 2012 | |
| **6. Network Passwords Requirements**<br>[redacted] | [redacted] | [redacted] | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| [redacted]<br><br>**Ranking: High** | [redacted] | [redacted]<br><br>**Responsible Officer:** Information Services Manager CUH / IT Technical Support Manager<br>**Implementation date:** Nov 2012 | The issues identified around passwords will be dealt with as part of key finding 1. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **7. IPMS User Access Management**<br>[redacted]<br>**Ranking: High** | [redacted] | [redacted]<br>**Responsible Officer:** Information Services Manager CUH / IT Technical Support Manager<br>**Implementation date:** Dec 2012 | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **8. Sensitive Data Accessible on Shares**<br>[redacted]<br>**Ranking: High** | [redacted] | [redacted]<br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Dec 2012 | Response to key finding 4 applies. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **9. ICT Budgeting**<br>At present no formal budget is prepared by ICT or by the hospital on the basis of existing commitments and known expenditure and at the date of the audit (March 2012) no ICT budget had been established for 2012, inter alia:<br>• Contracts and thus commitments in place;<br>• Ongoing maintenance;<br>• Hardware and/or software upgrades;<br>• Projects already committed to.<br><br>Thereby establishing what if any discretionary spend is feasible and the manner in which ICT expenditure can be financed.<br><br>We appreciate that project budgets are prepared an in addition a periodic cost containment meeting is chaired by the CEO of CUH to examine costs and the manner in which costs can be reduced and/or allocated.<br><br>The 2011 nominal ICT target budget was €658k and actual expenditure was in fact €1.217m.<br><br>In addition, it is apparent that a number of specific ICT expenditure items are not accounted for under the ICT budget and it is not clear if they are reported under the | The full and accurate cost of ICT may not be accurately captured and in addition accurately report to CMOD. | An ICT Budget should be prepared on the basis of existing commitments and known expenditure and it should include at a minimum the following, inter alia:<br>• Contracts and thus commitments in place;<br>• Ongoing maintenance;<br>• Hardware and/or software upgrades;<br>• Projects already committed to.<br><br>In particular, management should ensure that all ICT expenditure items are accounted for under the ICT Budget and reported under the ICT Expenditure - Start of Year Submission' (to the ICT Control Section, CMOD, Department of Finance) by National ICT. | CUH ICT will engage with CUH Finance to ensure that the budget reflects the requirements, in so far as is practical.<br><br>This is already in place and covered by annual submission to CMOD in Dept of Finance. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| ICT Expenditure – Start of Year Submission' (to the ICT Control Section, CMOD, Department of Finance) by National ICT e.g.<br>• Approximately €200k paid directly and via St. James's hospital relating to a Claimsure system in 2011 (procurement approach unclear);<br>• Payments made to AGFA (€300k approx. in 2011) relating to the use of the SAN, which was originally procured to support a radiology project but had been extended and is currently predominantly use as a key IT infrastructure component for the majority of CUH data.<br><br>**Ranking: High** | | **Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Dec 2012 | |
| **10.ICT Key Performances Indicators**<br>The auditor noted that there are no Service Level Agreements (SLA) agreed between the business and the ICT department. The ICT performances are not measured against specific / defined targets.<br><br>**Ranking: Medium (N)** | It may not be possible to identify if the service provided by the ICT department is adequate to adequately support the business and their business needs. | Management should define formal SLAs for the services provided by the ICT department to the business.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** N/A | In order to provide a SLA to the business community we would need to either have control over all of the components of the service or have a SLA with the units providing all of the components of the service. Neither of these case scenarios exist, and the first one will never exist. The provision of managed and measured SLA's for all components of all ICT services provided to the business community is not a task for which a timeline can be set at the moment. When SLA's are provided for HSE services |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | | external to CUH then this issue can be re-visited.<br><br>The identified risks and implications will be notified to the CUH Executive Management board and will be noted as risks.<br><br>No further action proposed. |
| **11.Reporting Structures, Roles and Responsibilities**<br>A lack of clarity between the roles and responsibilities of the local ICT department in CUH and the HSE South Region ICT department was apparent in the course of the audit.<br><br>Although meetings are held between the local ICT department within CUH and the HSE South Region ICT department, it appears that a formal reporting structure is not in place.<br><br>It was also understood that, although an operational draft ICT Strategy is being circulated between the HSE ICT South and the CUH ICT Department, the CUH ICT Department had little or no input into the HSE's National ICT Strategy.<br><br>**Ranking: Medium (N)** | The HSE's National ICT Management may not be aware of the local issues within the CUH ICT department, such as not adherence to the National HSE ICT Policies or the impossibility to achieve the ICT National objectives that would be drafted in the ICT Strategy.<br><br>In addition certain key ICT tasks may fall between stools due to a lack of clarity as to where responsibility lies. | Formal communications and reporting channels should be implemented between the local CUH ICT Department and the HSE's National ICT Department.<br><br>These should also allow for a formal assignment of responsibilities for the provision of ICT services, between the local, regional and National ICT Departments.<br><br>**Responsible Officer:**<br>Information Services Manager CUH | There is a good working relationship between the HSE and the CUH ICT services. We work in partnership on a range of projects and on on-going day to day issues. The implementation of formal roles and responsibilities has not been undertaken due to resource constraints as the ICT staff have concentrated on the delivery of an ICT service to the end users.<br><br>Two issues are specifically mentioned here;<br>1. Lack of clarity locally around roles and responsibilities. It was made clear during the course of the audit that there was no issue locally with this, but the audit view is different from the local view. In order to provide further clarity on this a Memorandum of Understanding will be |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | **Implementation date:** Sept 2012<br><br>**Responsible Officer:** Acting Head of National ICT / Information Services Manager CUH<br>**Implementation date:** March 2013 | drafted and agreed by all parties.<br><br>2. Formal communications channel between CUH ICT and HSE ICT. This is a matter for HSE ICT to address as it has implications for other hospital ICT departments also. CUH will work with HSE ICT on this and help to develop a communications framework between national ICT and hospital ICT departments. |
| **12. [redacted] Resilience**<br>Limited resilience is in place to protect CUH critical servers and data in the event of damage to the CUH data centre [redacted]<br><br>**Ranking: Medium (N)** | There is a risk of extended ICT services unavailability (i.e. CUH servers and data) if a damage affects the CUH data centre. | Management should ensure that resilience is established for the key ICT resources [redacted].<br><br>**Responsible Officer:** Acting ICT Tech Support Manager<br>**Implementation date:** Nov 2012 | A programme of work has commenced between CUH and the HSE South I&O to provide resilience on [redacted]. This involves the installation of hardware at both CUH and CFC and the use of a 'dark fibre' connection between the sites. The [redacted] Site Replication Manager software tool set will be used to achieve the required resilience. The server hardware has already been delivered to site. The full implementation will take substantial testing and will need to be fully documented. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **13.Notepad found in the CUH car park**<br>While this is an out of scope finding, the auditors are obliged to note and notify that a folder containing sensitive employee information was found by the auditors on the machine for paying the parking tickets.<br><br>**Ranking: Medium (N)** | Sensitive staff or patients' data may be disclosed in breach of the Data Protection Act(s). | Management should ensure that staff receive adequate training in relation to information security, and that they are aware of the risks associated with mismanagement of sensitive data.<br><br>Compliance testing should be carried out on a regular basis to reduce the risk of inappropriate behaviour.<br><br>**Responsible Officer:**<br>Information Services Manager CUH<br>**Implementation date:**<br>June 2012 | This has been notified to the relevant individual and Department and also to the HSE South Consumer Affairs Department (from a DP perspective).<br><br>Issue communicated on 29th May 2012.<br><br>No further action proposed. |
| **14.Intrusion Detection System (IDS)**<br>[redacted] | [redacted] | [redacted] | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| [redacted]<br><br>**Ranking: Medium** | [redacted] | [redacted]<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** July 2012 | [redacted] |
| **15.ICT Steering Committee**<br>Whilst an ICT Steering Committee is in place, the group would only appear to be project focused and does not provide oversight or review of:<br>• ICT standard performance metrics or targets;<br>• ICT operational budgets and reporting against budget;<br>• Data management and Data Protection;<br>• Security management;<br>• Policy compliance. | There is a risk that the ICT Steering Committee will not focus on or be aware of other ICT risks outside of project risk. | Management should expanding the range of topics addressed by the ICT Steering Committee to include subjects such as:<br>• ICT reporting processes (e.g. ICT application performance, security incidence, network | The existing ICT Steering Group has fulfilled the function set out initially which was around overall project governance and acting as a project board for a number of projects.<br><br>The current ICT Steering Group will be disbanded and a new ICT Governance Group with revised membership and revised terms of reference will be established within CUH. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **Ranking: Medium** | | issues and similar activities);<br>• Budgeting;<br>• Data Management;<br>• Security Management;<br>• Policy Compliance.<br><br>**Responsible Officer:** CEO CUH<br>**Implementation date:** Oct 2012 | |
| **16.Reporting on Policy Compliance or Exceptions**<br>A process to formally report on the implementation of, or compliance with, National ICT Security Policies is not in place.<br><br>Where non-compliance with the policies existed, these gaps had not been formally reported to the National ICT Directorate as required in the policies.<br><br>As a consequence, hospital management cannot provide an adequate level of assurance that the National ICT Security Policies are implemented, as requested by the HSE's CEO in his communication to all National Directors regarding Data Protection on the 10th August 2011. | The absence of an effective assurance process increases the risk of non-compliance with the National ICT Security Policies (which are critical to ensuring Data Protection compliance in respect to automated data) will go unreported.<br><br>As a consequence, senior management may not be fully aware of Data Protection risks until an | Management should consider the introduction of a formal report of the implementation of compliance with national ICT security policies.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** March 2013 | Such a reporting mechanism will be put in place and we will work with HSE ICT nationally on the practical implementation of these policies which are published without implementation plans and without associated technical resources being provided. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **Ranking: Medium** | incident occurs. | | |
| **17. Business Staff Awareness**<br>A number of business users were interviewed by the auditors to assess their knowledge of the Encryption, Remote Access, Access Control, and Passwords Standards National ICT Policies:<br>• 50% are not aware of any of the policies;<br>• 31% of users are aware of the existence of the policies but not their content;<br>• 19% are aware of and acknowledge having read, at most, one of the policies (Password Standards or Encryption).<br><br>100% informed the auditors that they have received no training in relation to any of the policies and have not been asked to accept them.<br><br>While the policies may be rolled out at a National level, there is little evidence to suggest they are being implemented at a local hospital level and user awareness of the contents and controls outlined in the policies is poor.<br><br>**Ranking: Medium** | In the absence of an appropriate level of end-user awareness of the National HSE ICT Policies there is an increased risk that a data breach or data security incident may occur resulting in reputational, financial and operational damage to CUH and the HSE. | A training and awareness programme related to the ICT policies should be established for business staff to promote the implementation of the ICT policies across the Organisation.<br><br>Management should consider the following:<br>• Using the existing training portal www.hseland.ie or an organisation-wide poster campaign to inform and update end-users on ICT policies;<br>• Establishing a user-awareness roadshow for delivering seminars on information security, ICT acceptable use and informing end- | As part of the revised ICT Governance framework, a programme of staff awareness will be undertaken. This is not a once off event so there is no completion date. The date below is the date on which it will commence. The manager's ICT Handbook will be a key part of this programme. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | users of the requirements of the approved ICT policies.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Jan 2013 | |
| **18.ICT Staff Awareness**<br>ICT staff have a mixed level of awareness of the National ICT Policies The audit found that although CUH ICT management and staff are aware that National ICT Policies exist, they are not aware of their content, the audit revealed that there is no direct communication of these policies to CUH ICT<br><br>Staff have had no training on the use and/or application of these policies and have not been asked to formally sign up to their acceptance of policies.<br><br>CUH ICT does not monitor the level of compliance with the policies and there is no requirement to report compliance levels to HSE ICT.<br><br>**Ranking: Medium** | In the absence of CUH ICT staff having a thorough and up-to-date knowledge of the ICT policies, there is a risk that services supported by CUH ICT may not be in line with HSE requirements. | A formal communication process to make CUH ICT staff aware of the National ICT Policies should be established. Management should also, on a regular basis, provide updates on policy requirements to staff and ensure that these requirements are understood and applied.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** July 2012 | This will be undertaken immediately. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **19.Active Directory Joiners Process Gaps**<br>There is no formal / documented User Access Management procedure that documents the process for creating active directory accounts and issuing network rights in line with HSE policy and business requirements. The National HSE Systems Access Request Form is not used to grant user access to the CUH network in line with the HSE Access Control Policy.<br><br>A local internet and email application form is in place within CUH that requires Line Managers' authorisation. However, the auditor tested a sample of new members of staff selected from a report provided by HR and determined that 13.3% of the forms were not authorised (i.e. not signed by Line Managers).<br><br>[redacted]<br><br>**Ranking: Medium** | There is a risk that unauthorised and inappropriate access could be granted to the CUH network where a defined User Access Management Policy is not in place that requires formal application and authorisation by a defined member of CUH prior to access being granted.<br>[redacted] | CUH should consider the development and implementation of a User Access Management procedure in line with the National HSE Policy standards that defines at minimum the following:<br>• Requirements for creating accounts;<br>• Defined list of authorisers;<br>• Defined list of authorisers for each shared drive;<br>• Defined list of who can authorised access to applications [redacted]<br>• Review process with HR ensure that access is revoked when members of staff either leave or no longer require access;<br>• Review of shared folder with business | This will be put in place. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | owner on a periodic basis to ensure that access is in line with business requirements;<br>• Review of [redacted] access to applications with systems owners to ensure that only members of staff that require access can run applications via [redacted]<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Oct 2012 | |
| **20.Leavers Process Gaps**<br>A formally documented procedure for revoking the access of leavers and movers is not in place.<br><br>A process is in place to disable all accounts that have been inactive for a period of [redacted] days or more; however, this process is not in line with the Access Control Policy which indicates that: "User access accounts which have been inactive for [redacted] consecutive | There is a risk that members of staff may continue to have access to patient data when they no longer require it. This may result in breach of Data Protection legislation. | A formal process should be developed to ensure that all CUH accounts (both network and applications accounts) are disabled as soon as a member of staff leaves the Organisation. This process should include a notification process from | We will establish such a procedure in conjunction with HR. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| days or more must be suspended unless instructed otherwise by the user's line manager."<br><br>[redacted]<br><br>**Ranking: Medium** | | HR.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Oct 2012 | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **21.Movers Process Absence**<br>A process is not in place in CUH to ensure that network access such as [redacted] shared folders and specialist applications granted to a member of CUH staff is revoked when they change role within the hospital.<br><br>**Ranking: Medium** | There is an increased risk that Hospital staff may have inappropriate or unauthorised access to personal and personal sensitive patient data potentially leading to a data breach impacting the reputation of the hospital. | A formal process should be developed to ensure that when a staff member moves within the Organisation, his/her previous level of access (e.g. application profiles, shares access) is removed unless otherwise specified before new access is granted.<br><br>Movements within the Organisation should be tracked, for example by the HR department, to allow audit and regular reviews.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Oct 2012 | We will establish such a procedure in conjunction with HR. |
| **22.AD Generic Accounts**<br>[redacted] | [redacted] | [redacted] | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| [redacted]<br><br>**Ranking: Medium** | [redacted] | [redacted]<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Dec 2012 | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **23.AD Administrators**<br>[redacted]<br>**Ranking: Medium** | [redacted] | [redacted]<br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** July 2012 | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **24.Active Users Reviews**<br>The threshold for identifying inactive accounts is not in line with the HSE Access Control Policy threshold of [redacted] days. [redacted] accounts were identified as being inactive for over [redacted] days.<br><br>While a process is in place for removing inactive accounts, through substantive testing the auditors were able to determine that [redacted] accounts have been inactive for over [redacted] days and have not been moved to the Disabled OU (Organisational Unit).<br><br>**Ranking: Medium** | There is a risk that inactive accounts are not being correctly disabled which may result in leavers / movers / absentees retaining an active account with varying levels of access to potentially sensitive information. This risk is increased if IT has a limited oversight of the leaver / mover process or receives limited notification from HR. | The Organisation should reduce the threshold for identifying inactive accounts to [redacted] days to be in line with HSE policy and ensure that the process of disabling inactive accounts is run regularly.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** March 2013 | The identification of leavers / movers is key to this. If we have a leaver and the account goes inactive we have no issue. However, if we have a leaver and the account remains active, then this process will not identify that.<br><br>We will strive to improve this process, however this requires an input of resources and we have already identified the very limited resource pool within which we are operating. |
| **25.Users' Access Rights Reviews**<br>A formal process for the review of the level of access granted to users is not in place within CUH. The auditor was unable to identify information owners for each department who are responsible for reviewing access rights within their department.<br><br>This does not meet the requirements of the HSE Access Control Policy that states:<br>Information owners or their nominees must continually monitor access to their information systems. They must | There is a risk of inappropriate or unauthorised access to network resources within a department where formal review of access rights are not carried out with individual department management. | CUH management should develop a formal network access review process in line with the National HSE Access Control Policy.<br><br>Information owners should be identified for all departments and systems and their roles and responsibilities clearly | This is linked to key finding 40 - Service Catalogue and to key finding 2 - Information Governance.<br><br>This will also be included the manager's ICT Handbook. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| perform quarterly reviews of the systems they are responsible for, to ensure:<br>• That each user access account and the privileges assigned to that account are appropriate and relevant to that users current role or function;<br>• The information systems and the information processed by the systems is only access and used by authorised users for legitimate reasons.<br><br>**Ranking: Medium** | | defined.<br><br>Quarterly reviews should be carried out with information owners to ensure that access to the network (e.g. shared drives) and applications [redacted] is only granted in line with the departments business requirements.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** March 2013 | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **26.Third Party AD Administrators**<br>[redacted]<br>**Ranking: Medium** | [redacted] | [redacted]<br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** July 2013 | [redacted] |
| **27.IPMS Administrative Access**<br>[redacted] | [redacted] | [redacted] | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| [redacted]<br>**Ranking: Medium** | [redacted] | [redacted] | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | [redacted] | [redacted] | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | [redacted]<br><br>**Responsible Officer:** HSE IPMS Team<br>**Implementation date:** Dec 2012 | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **28.IPMS Data Extraction Facilities**<br>[redacted]<br>**Ranking: Medium** | [redacted] | **Responsible Officer:**<br>Information Services Manager CUH<br><br>**Implementation date:**<br>Usage analysis / encryption: Aug 2012<br>Review use of alternate tools: Dec 2012 | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **29.Network Audit Logs**<br>[redacted]<br>**Ranking: Medium** | [redacted] | [redacted] | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | the logs);<br>• [redacted]<br>[redacted]<br>**Responsible Officer:**<br>Information Services Manager CUH / IT Technical Support Manager<br>**Implementation date:** July 2012 | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **30.Server Security Patches**<br>[redacted]<br>**Ranking: Medium** | [redacted] | [redacted]<br>**Responsible Officer:** IT Technical Support Manager<br>**Implementation date:** Oct 2012 | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **31.Use of USB keys**<br>[redacted]<br>**Ranking: Medium** | [redacted] | [redacted]<br>**Responsible Officer:** Acting Head of ICT Services / AND ICT I&O<br>**Implementation date:** Sept 2012 | [redacted] |
| **32.Presence of Possible Duplicates**<br>Data analysis was performed on the merged PAS databases of the CUH, South Infirmary and Mercy Hospitals. The data analysis performed on over 1.241 million records indicates the presence of 239,594 possible duplicate records (19.30% of the total) that need to be analysed by the Medical Records staff to assess whether these records could be merged or not. These duplicates were identified with a 3 Points Match:<br>1. Forename (exact forename or "sounds like" forename);<br>2. Surname (exact surname or "sounds like" | It may not be possible to correctly identify all IPMS accounts (and hence to retrieve all medical information) related to a patient. Key information may consequentially not be made available to medical staff and this may lead to incorrect patient medical care. | Management should consider the approval and implementation of the project proposed for the identification and clean-up of the duplicates in place within the IPMS:<br>• The medical record department should allocate resources to analyse the IPMS records that could | The HSE South IPMS Project Team submitted a Data Quality Improvement Plan to the Project Board and Area Manager in Dec 2011. Approval for this plan was given in May 2012 and July 2012 has been set as the start date for this. The plan has a 12 month time frame. This plan was made available to the auditors and does not need to be detailed here. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| surname);<br>3. Valid date of birth (DoB).<br><br>The auditors acknowledge that a similar process was carried out by local management; a proposal was drafted and at the time of audit this was being reviewed.<br><br>**Ranking: Medium** | | potentially be duplicates (e.g. records identified as duplicates based on the 3 Points Match);<br>• The identified duplicates should be merged.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Aug 2013 | |
| **33.Data Collection Process**<br>The data analysis performed on over the 22,302 records entered in IPMS after the data migration process was completed shows the presence of records that appear to be duplicates or that do not contain all key fields filled-in, the auditors used the 1st August 2011as a cut-off day. It appears that 5,530 records (33%) entered after the date of data migration contain errors.<br><br>This indicates that the duplicate identification process and the data collection process needs to be improved. The issues identified could be summarised as follows: | It may not be possible to correctly identify all IPMS accounts (and hence to retrieve all medical information) related to a patient. Key information may consequentially not be made available to medical staff and this may lead to incorrect patient medical care. | The process of collecting the data from patients should be improved to ensure that:<br>• The new records entered in IPMS allow for a correct identification of patients;<br>• New duplicate records are not entered;<br>• All key fields necessary | Response to key finding 32 applies. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| A. Errors, i.e. records that do not allow the identification of a patient (32 records, 0.14%);<br>B. Duplicates identified with a 4 Points Match (173 records, 0.78%);<br>C. Duplicates identified with a 3 Points Match (544 records, 2.44%);<br>D. Poor quality of the information collected by staff for 4,781 records (28,51% of the new records) which were identified based on the following analysis:<br>i. Forename or surname which length is no more than a character (12 records, 0.15%);<br>ii. Alive (i.e. there is no date of death) patients over 100 years old (poor reliance could be posed to these records – 3 records, 0.04%);<br>iii. Empty address line 1 (usually a street or road – 4 records, 0.05%);<br>iv. Empty address line 2 (usually the city – 48 records, 0.6%);<br>v. Empty phone number field (4,597 records, 57.97%);<br>vi. Invalid phone number field (117 records, 1.74%).<br><br>**Ranking: Medium** | | to identify a patient are entered in IPMS for both existing patients and new patients, they should be at least:<br>o Forename;<br>o Surname;<br>o Date of birth;<br>o Address line 1 (street/road);<br>o Address line 2 (city);<br>o Phone number.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Aug 2013 | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **34.ICT Helpdesk Performance**<br>The performance of the CUH ICT Helpdesk is not measured. CUH ICT management informed the auditor that 3 SLAs exist between ICT and:<br>• Bantry General Hospital;<br>• Mallow General Hospital;<br>• Blood Transfusion Service.<br><br>The auditor was also informed that ICT is not formally committed to respond to issues with defined times and service standards. However, they endeavour to return service in the best possible time frames.<br><br>Service desk performance statistics/reports are neither produced nor communicated to Senior Management.<br><br>**Ranking: Medium** | There is a risk that the ICT Helpdesk may not be able to adequately support the CUH business in line with their needs. As a result the medical staff may not be able to carry out critical hospital tasks. | SLAs between CUH ICT Helpdesk and the business should be defined and agreed for the helpdesk support of critical CUH systems and applications. Where the current resources will not facilitate the expected service level from the business a cost benefit analysis should be carried out.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** July 2012 | In order to provide a SLA to the business community we would need to either have control over all of the components of the service or have a SLA with the units providing all of the components of the service. Neither of these case scenarios exist, and the first one will never exist. The provision of managed and measured SLA's for all components of all ICT services provided to the business community is not a task for which a timeline can be set at this time.<br><br>When SLA's are provided for HSE services external to CUH then this issue can be re-visited.<br><br>The identified risks and implications will be notified to the CUH Executive Management board and noted as risks.<br><br>The SLA's identified are in place to satisfy external inspection of those areas and are not used as performance indicators.<br><br>No further action proposed. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **35.Network Segmentation**<br>[redacted]<br>**Ranking: Low (N)** | [redacted] | [redacted]<br>**Responsible Officer:** Information Services Manager CUH / Network Manager<br>**Implementation date:** July 2012 | [redacted] |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | | [redacted] |
| **36.ICT Steering Committee Meetings**<br>The auditors obtained copies of two ICT Steering Committee meeting minutes and noted that these documents contains only the agenda of the meeting and the agreed points. It appears that the following details are not formally documented:<br>• Details of the members that attended the meeting;<br>• Indication of who took responsibility for performing the agreed actions;<br>• Deadlines for implementing the agreed actions.<br><br>**Ranking: Low** | The points / actions identified during the ICT Steering Committee meetings may not be implemented timely due to lack of ownership and ambiguity of deadlines agreed. | Management should consider documenting the ICT Steering Committee Meetings in a more comprehensive manner to include at least the following:<br>• Details of the members that attended the meeting;<br>• Points discussed and actions agreed;<br>• Indication of who took responsibility for performing the agreed actions;<br>• Deadlines for implementing the agreed actions.<br><br>**Responsible Officer:** CEO | Response to key finding 15 applies. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| | | CUH<br>**Implementation date:** Oct 2012 | |
| **37.Network Issues Notification Emails**<br>Review of the network monitoring tools in place in the [redacted] (supporting the CUH network infrastructure) identified that the monitoring tools are configured to send notification emails in the event of a network performance issue or availability issue; however, these emails are only sent to an individual's mailbox rather than a group mailbox accessible by the rest of the team.<br><br>**Ranking: Low** | There is a risk that network issues are may not be identified and reacted upon in a proactive manner, where email notifications are not distributed to all members of the network support team. This risk is reduced due to the visual displays and audible alerts that are in place within the Network support teams' office environment. | The Network Manager should consider either implementing a Network Support Group mailbox or distributing email notifications to all members of the Network Team.<br><br>**Responsible Officer:** Information Services Manager CUH / Network Manager<br>**Implementation date:** July 2012 | During core working hours there is constant monitoring of network notifications.<br><br>The issue with e-mail notification is only relevant to the out-of-hours scenario. There are resource constraints within this unit which are further constrained out of hours where only one member of the team is in a position to receive notifications. This is why the e-mails only go to one person.<br><br>No further action proposed. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **38.Network Availability & Capacity Requirements**<br>[redacted]<br>**Ranking: Low** | [redacted] | [redacted]<br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** July 2012 | [redacted] |
| **39.Data Migration Issues**<br>Although a data clean-up process took place prior to and after the data migration steps, a number of issues were identified by analysing the data extracted from the IPMS system. | It may not be possible to correctly identify all IPMS accounts (and hence to retrieve all medical information) related to a patient. Key information | The ICT staff should perform a review of the IPMS records to:<br>• Inactivate the records that do not allow the identification of | Response to key finding 32 applies. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| The data analysis performed over 1.241 million records shows the presence of 49,517 records (3.99%) that should have been addressed as part of the data migration project. These exceptions could be summarised as:<br>A. Errors, i.e. records that do not allow the identification of a patient (3,297 records, 0.27%):<br>i. both forename and surname are not more than a character long;<br>ii. the date of birth is not valid plus it indicated an invalid forename or surname (e.g. it is empty, or equal to "downtime", "upgrade" or "unknown");<br>B. Duplicates identified with a 4 Points Match (46,220 records, 3.72%):<br>i. Forename (exact forename or "sounds like" forename);<br>ii. Surname (exact surname or "sounds like" surname);<br>iii. Valid date of birth (DoB);<br>iv. Address first line (if available) or Phone number (if available).<br><br>**Ranking: Low** | may consequentially not be made available to medical staff and this may lead to incorrect patient medical care. | patients;<br>• Merge the records that are reasonably identified as duplicates (e.g. where a 4 Point Match is identified).<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Aug 2013 | |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **40. Applications Identification**<br>A service catalogue is not in place for the identification of all applications used within CUH, with the details of:<br>• Business owners;<br>• System administrators;<br>• Sensitivity of the data held within the system.<br><br>**Ranking: Low** | There is a risk that all the applications and services provided to the business by ICT may not be identified. | Management should identify and formally document all applications / systems used within CUH into a service catalogue.<br><br>The catalogue should include at a minimum the following information:<br>• Business Owner;<br>• System Administrator;<br>• Sensitivity of the data held within the system.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Dec 2012 | A service catalogue and associated management and governance arrangements will be documented for review and endorsement by revised ICT Governance Group. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **41. Laptops Encryption**<br>A total of 24 laptops were sampled by the auditors and 6 were found unencrypted (25%); however, these unencrypted laptops could not get access to the HSE Network.<br><br>In fact, there is a process in place to block and log all unencrypted laptops that attempt to connect to the CUH network. Review of the log obtained identified that:<br>[redacted]<br><br>**Ranking: Low** | The presence of unencrypted laptops may lead to non-compliance with the National HSE Policy. In addition, even if not connected to the network, sensitive information could be stored in these laptop using other methods (e.g. by using USB keys) and if the laptop goes missing it may result in a Data Protection breach. | CUH should conduct a full review of all laptops in operation within CUH to ensure that they are all encrypted. This process should include a periodic review of the blocked laptop log to ensure the all laptops that attempt to connect are encrypted.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** Aug 2012 | Unencrypted laptops cannot gain access to network.<br><br>A review of unencrypted laptops will take place based on information provided by auditors and will be corrected.<br><br>Review of notifications carried out in early June identified no unencrypted laptops attempting to connect to the network. |

| Key Findings | Possible Implications | Recommendations | Management Response |
|---|---|---|---|
| **42.Smartphones Security**<br>At the time of the audit the auditor was informed that a maximum of [redacted] smart phone devices that have the capability of storing confidential or personal data were in operation and not encrypted. The auditor acknowledges that a new [redacted] solution is currently being evaluated.<br><br>**Ranking: Low** | There is a risk of breach of Data Protection legislation where devices that have the capability of storing confidential or personal data are not encrypted. This could have a significant impact on the reputation of CUH if such a device was to be found by the public. | CUH should consider the removal of all unencrypted mobile email devices and continue with the implementation of the new secure solution once fully tested.<br><br>**Responsible Officer:** Information Services Manager CUH<br>**Implementation date:** July 2012 | These devices have been removed from service as planned and replaced with devices that are managed and monitored using [redacted] Solution.<br><br>No further action required. |